Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-3 (canceled)

Claim 4 (currently amended): A system to provide a remote computing client access to resources provided by at least one server in at least one target computing network, comprising:

a point of presence node communicatively ~~connected~~ configured to connect to the at least one target computing network; ~~and~~

at least one Internet Protocol Security concentrator resident in the point of presence node;

at least one access server resident in the point of presence node, wherein the at least one access server comprises a virtual private network module ~~which implements~~configured to implement a secure communication channel between the remote computing client and the at least one server in the at least one target communication network.

Claim 5 (currently amended): The system of claim 4, wherein the remote computing ~~device~~ client comprises a virtual private network module ~~which~~ configured to cooperate~~s~~ with the virtual private network module resident in the point of presence node.

Claim 6 (currently amended): The system of claim 5, wherein:

the virtual private network module in the remote computing client communicates with the virtual private network module in the at least one access server using a message exchange mode; and

the virtual private network module in the remote computing client receives application layer data from at least one application executing on the remote computing client.

Claim 7 (currently amended): The system of claim 6, wherein the virtual private network module in the at least one access server is configured to implements a proxy client for at least one application executing on the remote computing ~~device~~client.

Claim 8 (currently amended): The system of claim 5, wherein the virtual private network module in the remote computing client and the virtual private module in the at least one access server are configured to establish an encrypted communication channel between a specific application executing on the remote computing client and the point of presence node.

Claim 9 (currently amended): The system of claim 8, wherein the virtual private network module in the remote computing client is configured to:

generate~~s~~ a first encryption data set comprising a public portion and a private portion; and

transmit~~s~~ the public portion of the first encryption data set to the virtual private network ~~server~~ module in a session set-up message.

Claim 10 (currently amended): The system of claim 5, wherein the remote computing device further comprises a reconfiguration system module ~~which~~ configured to collect~~s~~ system configuration data relating to the remote computing device, generate~~s~~ a system configuration file, and store~~s~~ the system configuration file in a memory module in the remote computing device.

Claim 11 (currently amended): The system of claim 10, wherein the at least one access server comprises:

a central policy manager module ~~that~~ configured to establish~~es~~ configuration policies for one or more remote clients that access resources via the virtual private network ~~server~~module; and

a reconfiguration system module ~~that~~ configured to cooperate~~s~~ with the reconfiguration system module in the remote computing device to impose configuration changes on the remote computing device.

Claim 12 (currently amended): The system of claim 10, wherein the reconfiguration system is configured to implements an atomic reconfiguration process on the remote computing device.

Claim 13 (previously presented): The system of claim 5, wherein the remote computing device comprises a local proxy module that emulates an HTTP proxy server.

Claim 14 (currently amended): The system of claim 10, wherein the remote computing device comprises a client application tunneling module, wherein the client application tunneling module is configured to extracts destination IP addresses and port numbers from communication packets and invokes the reconfiguration system module to reconfigure a name-to-address mapping for communications between the remote computing device and an application executing on a remote server.

Claim 15 (currently amended): The system of claim 5, wherein at least one server in the point of presence node further comprises a network address translation module that configured to performs network address translation on incoming and outgoing packets to enable remote access to resources on one or more networks outside the at least one target computing network.

Claim 16 (currently amended): The system of claim 15, wherein the network address translation module is configured to automatically determines a network configuration for the at least one target computing network.

Claim 17 (currently amended): The system of claim 5, wherein:

the at least one access server comprises a first network backup module;

the remote computing device client comprises a second network backup module; and

the first network backup module and the second network backup module are configured cooperate to back up and restore one or more files from the remote accessat least one server.

Claim 18 (currently amended): The system of claim 17, wherein the first network backup module is configured to maintains incremental backups of files used by the remote computing ~~device~~client.

Claim 19 (new): A method comprising:

receiving a public portion of a first encryption key value set from a client in a first session setup message;

generating a second encryption key value set corresponding to the first session setup message;

transmitting a public portion of the second encryption key value set in a second session setup message; and

if decryption of the second encryption key value set is successful by client, initiating a WTP session with the client with a shared encryption key.